Contenuti

- **Architettura di Internet**
- **Principi di interconnessione e trasmissione**

Tecnologie delle reti di calcolatori

- **World Wide Web**
- **Posta elettronica**
- **Motori di ricerca**

Servizi Internet (*come funzionano e come usarli*)

- **Antivirus**
- **Personal firewall**

Servizi Internet (*come difendersi*)

Introduzione alla sicurezza

Come comportarsi, quali sono i rischi e come difendersi

- Nell'uso della posta elettronica
- Nell'uso del Web
- Nell'uso di altri servizi di rete

Premessa

- Ci sono più di 300 milioni di utenti dei servizi Internet
- Tutti, potenzialmente, possono comunicare con il TUO computer collegato

- E, soprattutto, ciascuno di questi utenti può bussare alle "porte" del tuo computer per vedere se qualcuna è aperta

Riflessione

- Come cambierebbe il tuo comportamento (nel mondo) se sapessi che il tuo portafoglio, la tua casa e la tua cassetta della posta fossero accessibili a tutti, così come il tuo computer collegato ad Internet?

Possibili conseguenze di un "computer compromesso"

1. Conseguenze sul tuo computer
   - Difficoltà operative
   - Controllo/furto/danneggiamento di e-mail e documenti
   - Controllo e possibilità di transazioni finanziarie illecite (a tuo nome)
   - Furto di identità (nuova frontiera negli USA!)
2. Uso criminale del tuo computer per altri fini (*potrebbe essere penalmente rilevante*)

Come te ne accorgi

Vedi sul monitor ...

- Uno schermo blu, oppure figure strane o messaggi incomprensibili, ovvero messaggi di errore di sistema

Sperimenti…

- Ritardi inusuali nell'accensione del computer
- Computer che "va estremamente lento"
- Vi sono (molti) file corrotti, inaccessibili o mancanti
- Non riesci ad accedere ai tuoi dati sul disco o al disco stesso
- Il computer ha improvvisi (e frequenti) messaggi di memoria insufficiente
- Perdi completamente il controllo del tuo computer

Ma potrebbe anche darsi che non sperimenti alcun sintomo e sei del tutto inconsapevole che il tuo computer è stato compromesso

Possibili conseguenze

Case Study

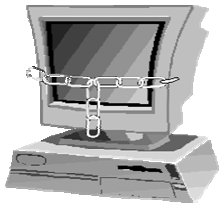
- **Dr. Porter installed a powerful new operating system on his computer and connected it to the Internet before applying the necessary patches**
- **His machine was hacked within 30 minutes**
- **The hacker inserted software that corrupted his hard disk**
- **He lost years of scientific work, his historical email archives, and a research manuscript**

La buona notizia

La maggior parte di incidenti può essere prevenuta

Cosa fare?

- Essere preparati a:
  - **Proteggersi ("Protect")**
  - **Riconoscere ("Detect")**
  - **Reagire ("React")**



Se non tu, chi?
Se non ora, quando?

Errori comuni

- Uso di password “banali”
- Lasciare incustodito il computer acceso
- Aprire allegati di e-mail da sconosciuti
- Non installare software anti-virus
- Perdere (anche temporaneamente) il portatile
- Condividere informazioni (password e account)
- Non riportare violazioni di sicurezza
- Non aggiornare il sistema operativo (patches) e il software antivirus

Account e Password: FARE

- Scegliere una password che non può essere indovinata (es., un acronimo di una frase con qualche numero inserito a caso)
- Cambiare la password almeno 2-4 volte all’anno
- Spegnere il computer alla fine della giornata
- Usare il desktop locking durante il giorno (es., uno screen saver con password per il ri-accesso)
- Cambiare la password anche se si ha un minimo sospetto che qualcuno l’abbia vista o sentita

Account e Password: NON FARE

- Diffondere la password (MAI dare la propria password al telefono, neanche ad Help Desk o assistenza!)
- Consentire a qualcuno di accedere con il tuo account+password
- Scrivere la password e attaccarla con Post-It sulla tastiera, mouse-pad, monitor, o portapenne
- “Save this Password” nel browser (Chiunque con accesso al tuo computer potrebbe “impersonificare te”)
- Cercare informazioni “sensibili” per conto di altri che non ne sarebbero autorizzati e tanto meno farlo per persone al telefono!

Back up

- Salvare periodicamente (almeno) i file più importanti su supporto diverso dal disco fisso usato normalmente, in modo che possano essere ripristinati nel caso si verificassero perdite o danneggiamenti di dati
- Se possibile, salvare i file su di un disco accessibile via rete che viene “backuppato” (backed up) frequentemente
- Verificare periodicamente l’integrità dei file di copia salvati (per evitare brutte sorprese…)

Uso della posta elettronica

Sicurezza nell'e-mail: FARE

- Installare e usare software anti-virus, e (soprattutto) mantenerlo aggiornato – giornalmente o settimanalmente
- Assicurarsi dal testo della mail, dallo scopo e dal mittente se è il caso di aprire un allegato (attachment)
- Segnalare all'assistenza tecnica tutte le e-mail con contenuti offensivi, osceni e che richiedono informazioni personali (su di te o su altri)
- Cancellare tutte le e-mail di pubblicità non richiesta SENZA RISPONDERE (no reply).
- RICORDARE che le istruzioni riportate "to remove you from the mailing list" spesso servono proprio come conferma che l'account di e-mail è funzionante

Sicurezza nell'e-mail: NON FARE

- Installare e usare software anti-virus, e (soprattutto) mantenerlo aggiornato – ogni giorno o settimana
- Aprire (*click on*) attachment o link Web inviati in e-mail di cui non si conosce la sorgente
- Conservare vecchie e-mail per sempre
- Considerare le e-mail diverse da una "cartolina". La e-mail NON è un messaggio privato, a meno che non sia crittografato
- Inviare identificativi e password in un messaggio di e-mail
- Inviare messaggi offensivi, insultanti, minacciosi, osceni, ecc.
- Inviare dati personali (es., nome, account, indirizzo di casa, foto) a qualcuno non noto personalmente

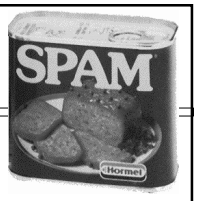
Aprire o no un attachment?

REGOLA: Se l'attachment è sospetto, non aprirlo!

PROBLEMA: Come rendersi conto che un attachment è sospetto?

- Se è collegato ad un e-mail che non è collegata a motivi di lavoro
- Attachment che non si aspettano
- Attachment con un'estensione sospetta (es., *.exe, *.vbs, *.bin, *.com, o *.pif)
- Un messaggio da parte di persona non nota che invita a "cliccare" su di un link Web

SPAM



- Origini da una scenetta del Monty Python Flying Circus (la carne in scatola Spam)

➔ Azione di diffondere in modalità broadcast (cioè, a tutti i possibili utenti di posta elettroncia) messaggi pubblicitari via e-mail

In generale, si considera SPAM qualsiasi e-mail non richiesta e non desiderata

- Consuma tempo (per eliminarla) e spazio su disco
- E' sempre fastidiosa, spesso offensiva, e talvolta contenente hoax o scam (si vedranno in seguito)
- Costa milioni di dollari ai grandi provider

Cosa può essere considerato Spam?

- Se ricevo notizie di una conferenza che mi interessa è spam?
- Volume e frequenza dei messaggi: quando diventa spam?
- …

Perché lo SPAM?

Basta fare un po' di conti …

- **Inviare e-mail spam a circa 100 milioni di mailbox**
- **Se anche solo il 10% legge la mail e clicca sul link ➔ si raggiungono 10 milioni di persone**
- **Se 1% delle persone che va sul sito, sottoscrive per esempio all'offerta di prova per 3 giorni ➔ (100,000 persone) x ($0.50) = $50,000**
- **Se l'1% della prova gratuita, si iscrive per 1 anno ➔ (1,000 persone) x ($144/anno) = $144,000/anno**

Cosa fare?

- NON RISPONDERE MAI NE' CHIEDERE DI ESSERE ELIMINATI DALL'ELENCO
- Non rispondere alle e-mail che richiedono dati personali
- Non comprare niente che ha origina da una mail spam
- Non contribuire a proposte di elemosina provenienti da mail spam
- Pensare due volte, meglio tre, prima di aprire un attachment
- Non inoltrare messaggi di "catene di e-mail"
- Controllare se l'ISP ha in atto provvedimenti o spazi adatti per la gestione dello spam

  ➔ USO DI PRODOTTI ANTISPAM

Proteggere il proprio indirizzo (*se possibile*)

- Utilizzare almeno due o tre indirizzi:
  - **Indirizzo privato**
  - **Indirizzo di lavoro**
  - **Indirizzo "commerciale"**
- Non divulgare il proprio indirizzo privato se non alle persone che si conoscono
- Utilizzare un indirizzo di e-mail dedicato esclusivamente alle transazioni/acquisti via Web
- Leggere bene le politiche utilizzate (se utilizzate e dichiarate…) dai vari siti per la gestione dei dati personali

Altri rischi

Rischi

- VIRUS
- HOAX
- PHISHING
- SPYWARE

Virus

- I virus informatici sono dei programmi (tipicamente molto piccoli) realizzati da …… che sono in grado di replicarsi e di diffondersi in modo autonomo da un computer all'altro
- I virus non sono nati o causati da Internet, ma certamente lo sviluppo di Internet ha aggravato il potenziale di diffusione

I primi sintomi di malfunzionamento o funzionamento diverso dal normale dovrebbe già mettere in allerta

- Come nel caso dei virus non informatici, l'intervento tempestivo è la medicina migliore

Alcuni tipi di virus

- Bomba logica: il virus si presenta come una qualsiasi applicazione informatica, ma ha al suo interno una funzione ostile che, tipicamente, si attiva dopo un certo tempo o al verificarsi di un determinato evento. Può essere molto distruttivo (es., cancellare l'intero contenuto del disco)
- Cavallo di Troia: Programma che è collegato ad un altro file innocuo, che viene scaricato o installato dallo stesso utente. Una volta installato sul computer, può avere vari effetti dannosi. Es.,
  - **Informare il creatore (o diffusore) quando si attiva una connessione Internet, consentendogli di accedere al computer stesso (in modo manifesto, distruttivo, o anche in modalità nascosta)**

SOLUZIONE

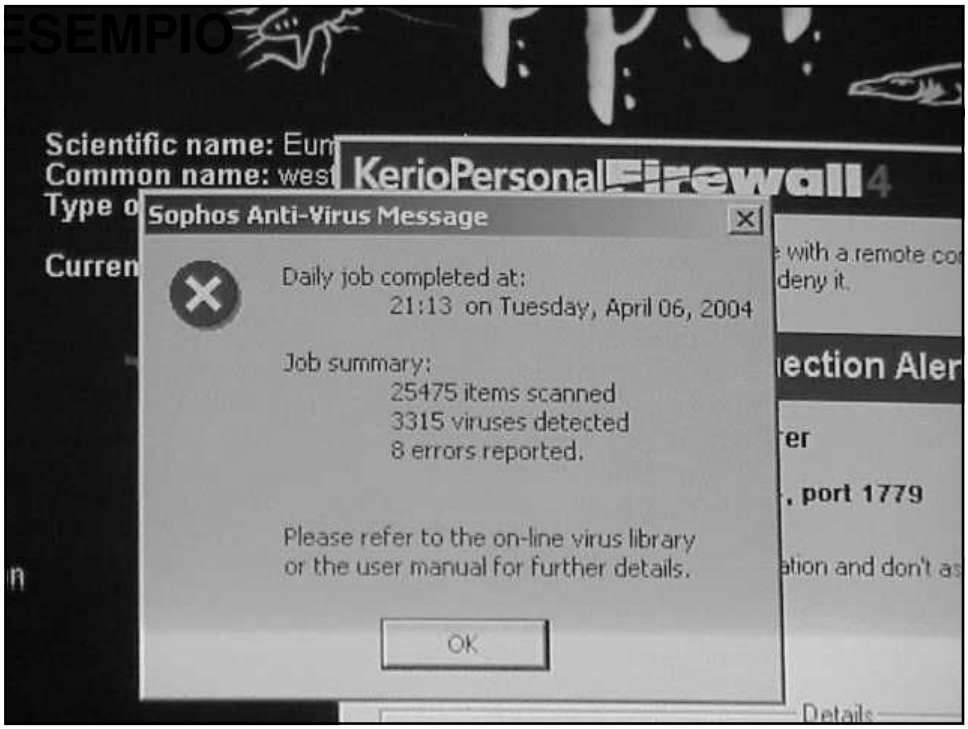
- NON CI SONO ALTERNATIVE!!!

  Bisogna installare un antivirus e bisogna tenerlo continuamente aggiornato.

  Non solo ma è poi fondamentale, se ciò non avviene in automatico, fargli eseguire periodiche scansioni sulle unità di memorizzazione principali (hd innanzitutto).

Azioni da compiere

- L'anti-virus è indispensabile sia per proteggere noi dagli altri sia per proteggere gli altri da noi
- Con la diffusione continua di nuovi virus, purtroppo, non si può essere mai sicuri che non si verrà infettati
- Tuttavia, si possono ridurre le probabilità di infettarsi
  →**Prendendo continuamente nuovi "vaccini"**
- La frequenza giornaliera nell'aggiornamento non è da "paranoici": è la medicina migliore!



HOAX

Chain Letters **(In Italia, nota anche come "Catena di Sant'Antonio") – Una mail che richiede al destinatario di inoltrarla al maggior numero di persone che conosce (spesso collegata a record, presunte opere caritatevoli, promozioni commerciali, …)**

Virus Hoax **– Un caso particolare del precedente: mail di allerta che avvisa di un nuovo pericolosissimo virus. Richiede all'utente di diffondere l'avviso al maggior numero di persone che conosce**

➔ **Il virus è la mail stessa! Non perché contiene un virus, ma perché tende ad intasare le mailbox**

False Alarms **– Un messaggio (volutamente errato) che indica che un certo file risulta infettato da un virus**

HOAX (*cont.*)

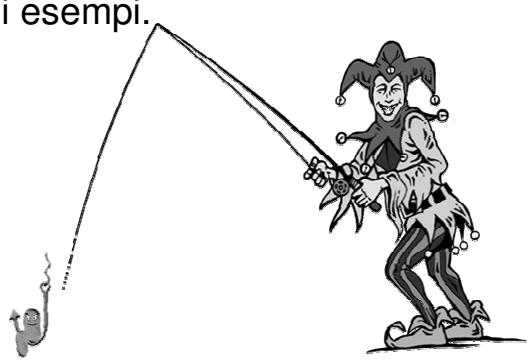
Misunderstandings **– Un problema che viene spesso attribuito erroneamente ad un virus informatico**

Scam **– Una proposta di business fraudulento**

Scare **– Un avviso di possibile rischio che viene intenzionalmente enfatizzato molto più del necessario**

Phishing

- Non è un virus, ma sono modalità fraudolente per ottenere informazioni personali
- Può capitare a chiunque…
- Vedere http://www.antiphishing.org per una interessante serie di esempi.



SPYWARE

- Spyware è un termine generale con cui si definisce certo software utilizzato per scopi fraudolenti con diversa rilevanza:
  - Reperire informazioni personali per scopi pubblicitari
  - Reperire informazioni (personali, password, numero carta di credito, software utilizzato, ecc.)
  - Modificare la configurazione del computer
  - Tracciare tutte le azioni o tracciare solo l'uso di determinati servizi Internet (es., pagine Web visitate)

  Tutto senza chiedere il consenso

Problemi con Spyware

- Software che raccoglie informazioni su di te e sull'uso del tuo computer
- Potrebbe anche essere vista come una cosa positiva. Es., Ti iscrivi ad un servizio di musica, lo spyware prende nota, e arriva molta più pubblicità di natuara musicale
- La maggior parte, tuttavia, sono molto negativi:

  raccogliere le password, numero di carte di credito, conto corrente, ecc.
- ESEMPIO

Programmi Toolbar → una volta installati, possono essere configurati per raccogliere qualsiasi informazione: tasti battuti, siti Web visitati, nomi e password

ANCHE SE VENGONO RIMOSSI, lasciano delle "briciole"

che consentono la re-installazione automatica

Problemi con Spyware

- Tutta l'informazione trasmessa via Web può essere intercettata (a meno di utilizzare connessioni sicure con trasmissioni cifrate)
- Alcuni siti, senza autorizzazione, sono in grado di aggiungersi al desktop, all'elenco dei siti preferiti, o addirittura sostituirsi alla homepage (hijacking)
- Tutta l'attività del browser può essere tracciata e monitorata
- Informazioni personali possono essere trasmesse o vendute a terze parti senza necessità di consenso e in modo del tutto inconsapevole
- Questi componenti malevoli non solo mettono a repentaglio la privacy, ma la stessa integrità del computer, oltre a diminuire l'efficienza (occupano spazio disco, memoria e rallentano le prestazioni)

Come accorgersi di avere uno spyware

- Si vedono pop-up pubblicitari che appaiono sullo schermo, anche quando non si sta navigando
- La home page del browser o altre opzioni sono state modificate senza consenso
- Si nota una nuova toolbar nel browser che non è stata installata esplicitamente e che non si riesce ad eliminare
- Il computer impiega più del necessario ad eseguire alcune operazioni
- Si sperimentano improvvisi crash del computer (es., blocco della tastiera o riavvio inaspettato del computer o di qualche applicazione)

Difese

- Installare ed eseguire uno dei seguenti prodotti anti-spyware

Spybot Search and Destroy
http://spybot.eon.net.au/index.php?lang=en&page=start

Ad-Aware (da Lavasoft)**
http://www.lavasoftusa.com/software/adaware/

****Gratuito per uso personale**

Consigli di base

1. Fare uso di software “anti-virus” avendo cura di tenerlo aggiornato
2. Non aprire allegati da e-mail di provenienza sconosciuta, inaspettata e/o sospetta
3. Utilizzare password di difficile decifrazione e cambiarla periodicamente
4. Proteggere il proprio pc da attacchi in arrivo da internet facendo uso di “firewalls”
5. Non condividere l’accesso al proprio pc con sconosciuti

Consigli di base (*cont.*)

6. Non lasciare il pc connesso a internet quando non necessario e soprattutto quando (da noi) non custodito
7. Eseguire periodicamente copie di back up dei propri dati e salvarle su supporti diversi dallo stesso hard disk del pc
8. Eseguire periodicamente download per tenere aggiornato oltre all’antivirus anche il sistema operativo (in particolare per windows!!)
9. Alla luce dei comportamenti “a rischio” elencati in precedenza evitarli o quanto meno ridurli al minimo
10. Condividere consigli e suggerimenti sulla sicurezza con famigliari, colleghi e amici

Firewall

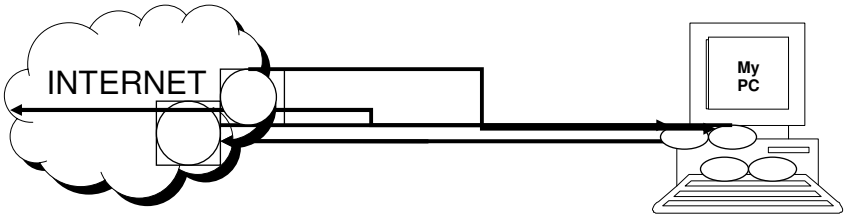
Fondamenti comunicazioni Internet

- La comunicazione via Internet si ottiene mediante lo scambio di molteplici “pacchetti” di dati
- Ogni pacchetto è trasmesso dal computer sorgente al computer destinazione
- La “connessione” è in realtà costituita da singoli pacchetti che viaggiano tra due processi in esecuzione su questi due computer connessi ad Internet
- Le macchine coinvolte “si accordano sulla connessione” e ciascuna di loro invia dei “pacchetti di servizio” (“ack”) che indicano al computer mittente che ha ricevuto correttamente i dati inviategli

Comunicazione tra processi

Ciascuna comunicazione è tra processi in esecuzione su computer. Pertanto, viene identificata dalla quadrupla:

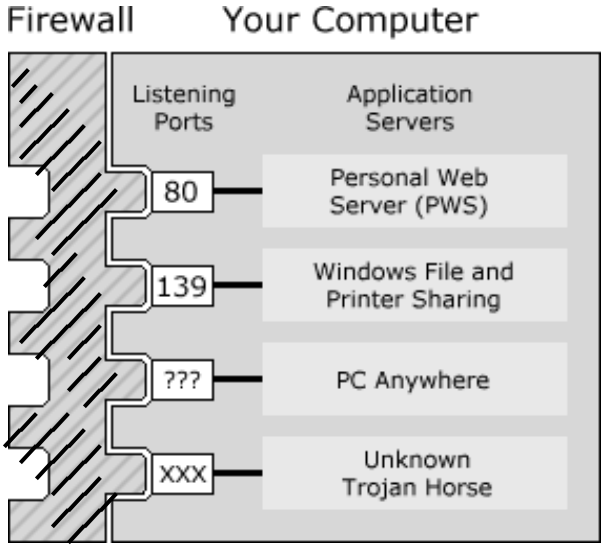
- ***indirizzo IP mittente***
- ***indirizzo IP destinatario***
- ***porta mittente***
- ***porta destinatario***



Cos'è un firewall?

- Un sistema di sicurezza (software o hardware + software) che agisce come una fascia protettiva tra una rete ed il mondo esterno di Internet
- Isola il computer da Internet utilizzando un "muro di codice"
  - **Ispeziona ciascun "pacchetto" in arrivo dall'interno o dall'esterno**
  - **Determina se lasciarlo passare o bloccarlo**

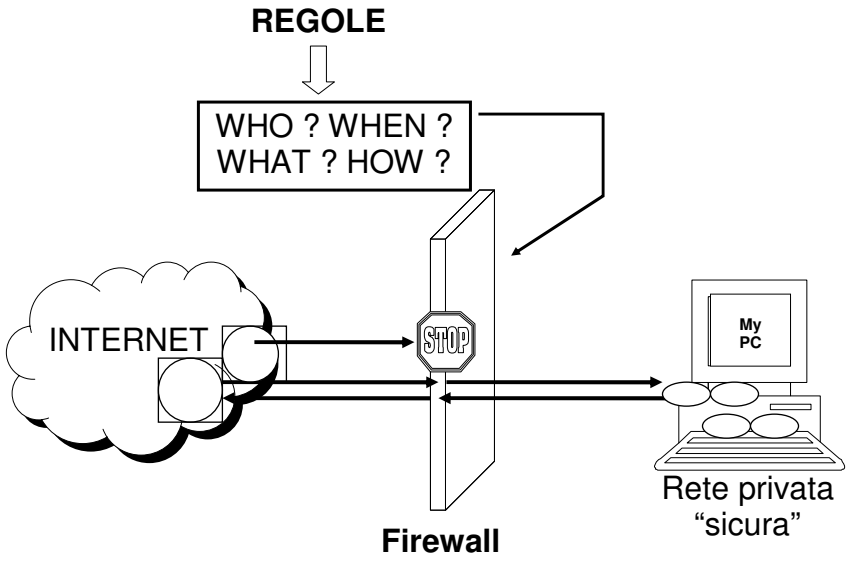
Posizione del firewall



Compiti di un firewall

- Il firewall è un software che ispeziona ciascun pacchetto non appena arriva alla macchina – PRIMA che il pacchetto venga trasmesso ad altro software che è in esecuzione sul computer
- Il firewall ha potere di veto totale su tutto ciò che il computer riceve da Internet
- Una "porta" TCP/IP è "aperta" sul computer solo se il primo pacchetto del mittente che chiede una connessione, riceve una risposta dal computer destinatario.
- Se, invece, la "porta è chiusa", il pacchetto in arrivo viene semplicemente ignorato e scomparirà da Internet. Significa che non è possibile utilizzare quel servizio Internet sul tuo computer

Come funziona



Efficacia del firewall

- Ma il vero potere di un firewall è strettamente collegato alla sua capacità di selezionare COSA LASCIAR PASSARE e COSA BLOCCARE
- Un firewall può "filtrare" i pacchetti in arrivo sulla base di varie informazioni:
  - Una qualsiasi combinazione di indirizzo IP della macchina mittente, della porta mittente e dell'indirizzo e della porta della macchina destinazione
- A tale scopo il software del firewall ispeziona l'informazione nell'header dei pacchetti (indirizzi IP e porte) entranti e, talvolta, uscenti. Sulla base di queste informazioni, il firewall blocca o trasmette i pacchetti.